QMARK 201.2

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s)	:	Shepherd, et al.
Serial No.	:	10/791,019
Filed	:	March 2, 2004
For	:	SECURE BROWSER
Examiner	:	Haoshian Shih
Art Unit	:	2173
Customer No.	:	10037

June 25, 2010

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

REPLY BRIEF UNDER 37 C.F.R. § 41.41

In response to the Examiner's Answer dated May 25, 2010, Applicants provide herewith their Reply Brief.

(vii) Argument.

REJECTION OF CLAIMS 1-21 UNDER 35 U.S.C. § 112. FIRST PARAGRAPH

Claims 1-21 are rejected under 35 U.S.C. § 112, first paragraph, as allegedly failing to comply with the written description requirement, and in particular, the use of the phrase "or a normal browser is to be employed" in claim 1, and "or whether an insecure browser is to be employed" in claim 9 are asserted by the examiner as failing to be supported by an adequate written description in the specification.

The Examiner apparently interprets claims 1 and 9 to require three distinct browsers, a "browser", a "normal browser" or an "insecure browser" and an "insecure browser". In fact, the claims require only two different browsers: an undistinguished or "normal browser" or "insecure browser" on one hand, and a "secure browser" on the other. It is respectfully submitted that this interpretation, which is consistent with the specification, does not render the claim insolubly ambiguous. Exxon Research and Engineering v. United States, 265 F.3d 1371, 1375 (Fed. Cir. 2001). See, United Carbon Co. v. Binney & Smith Co., 317 U.S. 228, 236 (1942) ("[t]he statutory requirement of particularity and distinctness in claims is met only when the [claims] [1] clearly distinguish what is claimed from what went before in the art and [2] clearly circumscribe what is foreclosed from future enterprise."); Marley Moulding Ltd. v. Mikron Industries, Inc., 417 F.3d 1356, 1359 (Fed. Cir. 2005) ("The statute [35 U.S.C. s. 112, [paragraph] 2] is satisfied if a person skilled in the field of the invention would reasonably understand the claim when read in the context of the specification."); Datamize, LLC v. Plumtree Software, Inc., 417 F.3d 1342, 1347 (Fed. Cir. 2005) ("Only claims 'not amenable to construction' or 'insolubly ambiguous' are indefinite." (citing Novo Indus., L.P. v. Micro Molds Corp., 350 F.3d 1348, 1353 (Fed. Cir. 2003); Honeywell Int'l, Inc. v. Int'l Trade Comm'n, 341 F.3d 1332, 1338 (Fed. Cir. 2003);

Exxon Research & Eng'g Co. v. United States, 265 F.3d 1371, 1375 (Fed. Cir. 2001))). See also, Memorandum from John Love, Deputy Commissioner for Patent Examination Policy, to Technology Center Directors and Patent Examining Corps (Sept. 2, 2008), available at http://www.uspto.gov/web/patents/memoranda.htm ("If the language of a claim, considered as a whole in light of the specification and given its broadest reasonable interpretation, is such that a person of ordinary skill in the relevant art would read it with more than one reasonable interpretation then a rejection of the claim under 35 U.S.C. 112, second paragraph, is appropriate.")

It is clear in claim 1 that the "browser" corresponds to the "normal browser, as follows:

> controlling the browser to request a document from a cooperative server, **the browser providing data export support functionality**; …
> automatically determining, based on a received data encoding type, whether a secure browser or a normal browser is to be employed, **the secure browser having a set of functionality restricted with respect to the normal browser, to enhance security of a received document against data export**;…

It is likewise clear in claim 9 that the "browser" of the preamble corresponds to the "insecure browser, as follows:

> 9. A secure user interface method, for interacting with a user through a browser, **the browser providing a set of navigational functionality**, comprising: …
> automatically determining, based on a received data type encoding, whether a secure browser is required to be employed by a content provider or whether an insecure browser is to be employed, **the secure browser restricting interaction of the user with tasks other than those permitted by the secure browser which are permitted by the insecure browser**;…

In each case, the distinction between the normal/insecure browser and the secure browser is a defined attribute of the "browser", and thus by the very terms of the claims, the "browser" itself falls within the scope of the normal/insecure browser.

It is therefore error to seek to interpret the claims without consideration of the specification, and thus to require three distinct browsers, as opposed to the selection of one of two types of browsers from an initial browser of unspecified but inherently defined type. Indeed, the examiner cites the language of the specification in defending his rejection, and thus it is clear that the Examiner knows that his own claim interpretation is inconsistent with the specification. Therefore, the rejection should be reversed.

REJECTION OF CLAIMS 1-4 AND 6-20 UNDER 35 U.S.C. § 102(e).

Claims 1-4 and 6-20 are rejected under 35 U.S.C. § 102(e) as being anticipated by Winneg et al., US 7,069,586.

The Examiner newly asserts that it is "common knowledge" that "data (password code) inputted in a computer in a first computer is first encoded/interpreted/mapped onto bytes (0's and 1's) in order for the computer [to] process/understand the inputted data."

It is initially noted that it is improper for the examiner to newly assert in his Answer such "common knowledge" as "evidence", without giving Applicant a full opportunity to respond to the alleged evidence in a non-final action. Applicants fully reserve all such rights, but take this preliminary opportunity to directly respond.

Claims 1 and 9 do not merely require that a password be "encoded", but rather that the secure application is invoked based on a "received data encoding type" (claim 1) or "received data type encoding" (claim 9). Using the Examiner's analogy, the encoding type or data type encoding of a "password" is always the same, whether or not the password is correct or incorrect or indicative of a particular privilege level. Therefore, Winneg et al. do not employ a "received data encoding **type**" (claim 1) or "received data **type** encoding" (claim 9) to invoke the secure application, but rather an analysis of the data itself, which is always of the same **type**, and therefore the "type" *per se* is irrelevant to any selective analysis performed by Winneg.

Note also that the user password is passed from the client to the server, while the data "type" is part of the information sent from the server to the client. Claim 1 specifically provides the step of "receiving data", and then "automatically determining, based on a **received** data encoding type, whether a secure browser or a normal browser is to be employed…". Likewise, claim 9 provides "receiving data in response to the request", and then "automatically

determining, based on a **received** data type encoding, whether a secure browser is required to be employed ..." Since the data is defined in the claim as being received, the received data encoding type or received data type encoding should be interpreted to apply to the received data, and not to some other data.

Therefore, it is respectfully requested that the rejections be reversed.

Respectfully submitted,

/Steven M. Hoffberg/
Steven M. Hoffberg
Reg. No. 33,511

HOFFBERG & ASSOCIATES
10 Bank Street-Suite 460
White Plains, NY 10606
(914) 949-2300